JOURNAL OF COMBINATORIAL THEORY, Series B 36, 135–155 (1984)

On the Minimum Order of Graphs with Given Semigroup

VÁCLAV KOUBEK AND VOJTĚCH RÖDL

Faculty of Mathematics and Physics, Malostranske nam. 25, 11800 Prague 1, Czechoslovakia and Faculty of Physical Engineering, Department of Mathematics, Husova 5, 11000 Praha 1, Czechoslovakia

Communicated by the Editors

Received August 31, 1981

Denote by $M(n)$ the smallest positive integer such that for every n-element monoid M there is a graph G with at most $M(n)$ vertices such that $\mathrm{End}(G)$ is isomorphic to M. It is proved that $\sqrt{2}(1+o(1))n\sqrt{\log_2 n} \leqslant M(n) \leqslant n \cdot \sqrt{2n} + O(n)$. Moreover, for almost all n-element monoids M there is a graph G with at most $12 \cdot n \cdot \log_2 n + n$ vertices such that $\mathrm{End}(G)$ is isomorphic to M.

INTRODUCTION

Let G, H be two graphs. A mapping $\varphi: V(G) \to V(H)$ is a homomorphism if $\{x, y\} \in E(G)$ implies $\{\varphi(x), \varphi(y)\} \in E(H)$. It is an old result of Hedrlín and Pultr, see, e.g., [16] that for every monoid M there exists a graph G such that the endomorphism monoid of G is isomorphic to M. It follows immediately from known constructions that if M is infinite there exists a G with the above property and such that $|G| = |M|$, see [16]. The problem of minimal representation of finite monoids appears to be much more difficult. It follows from an old construction of Hedrlín and Pultr, see [11], that every finite monoid with n elements has a representation by a graph with cardinality cn^2. It has been shown by Babai [1] that for every finite group G different from the cyclic groups Z_n, $n = 3, 4, 5$ there exists a graph H with at most $2|G|$ vertices and with automorphism group isomorphic to G. This led to the following problem, formulated first by Babai and Nešetřil, see [2].

Denote by $M(n)$ the minimum positive integer such that for every monoid M, $|M| \leqslant n$ there exists a graph G with at most $M(n)$ vertices having M as an endomorphism monoid. Is it true that $M(n) \leqslant cn$ for some $c > 0$?

In this paper we give a negative answer to this problem. We prove that

$$\sqrt{2}(1+o(1))\, n \sqrt{\log_2 n} \leqslant M(n) \leqslant \sqrt{2}\, n^{3/2} + \sqrt{72n}. \tag{1}$$

0095-8956/84 $3.00

A similar upper bound has been independently obtained by Babai [3]. He proved

$$M(n) \leqslant (2 + o(1))\, n^{3/2}.$$

Further, we investigate the class of 3-nilpotent monoids, i.e., monoids with a zero 0 (i.e., $x \cdot 0 = 0 \cdot x = 0$ for each x) and such that $x \cdot y \cdot z = 0$ if $x \neq 1$, $y \neq 1$, $z \neq 1$ (1 is the identity element of M). Note that from the result in [14] it follows that almost all monoids are 3-nilpotent. Denote by $N(n)$ the minimal positive integer such that for every 3-nilpotent monoid M with n elements there exists a graph with at most $N(n)$ vertices having M as an endomorphism monoid. Here, we show that

$$\sqrt{2}(1 + o(1))\, n \sqrt{\log_2 n} \leqslant N(n) \leqslant 12 \cdot n \cdot \log_2 n + n \tag{2}$$

and thus almost all monoids with n elements can be represented by a graph with $12 \cdot n \cdot \log_2 n + n$ vertices.

Another question which arises here is, what are the minimal orders of hypergraphs representing monoids? Let k be a positive integer $\geqslant 3$, denote by $M_k(n)$ the minimal positive integer such that for every monoid M on an n-point set there exists a k-uniform hypergraph G with at most $M_k(n)$ vertices such that the endomorphism monoid of G is isomorphic to M. We show that

$$M_k(n) \leqslant 3n \text{ for every } k = 3, 4, \ldots, \text{ and } n \geqslant 6k + 6.$$

The other type of questions studied in this paper are estimations of numbers of graphs with n vertices and a given endomorphism monoid. We focus on the situation when M is fixed and n is large. The important tool here is the following proposition.

Denote by u_n the largest t such that there exists a family $\{H_1, H_2, \ldots, H_t\}$ of graphs with n vertices which are pairwise rigid, i.e., such that

> if $\varphi: H_i \to H_j$ is a homomorphism then $i = j$
> and φ is an identity mapping.

We show that

$$u_n = \left(\begin{matrix} \binom{n}{2} \\ \left\lfloor \frac{1}{2} \binom{n}{2} \right\rfloor \end{matrix} \right) \cdot \frac{(1 + o(1))}{n!}$$

and moreover $\{H_1, H_2, \ldots, H_t\}$ can be chosen so that none of the H_i,

$1 \leqslant i \leqslant t$, contains a large clique, cf. Theorem 1.10. This result is used to prove that for a given monoid M there exist

$$\geqslant 2^{\binom{n-\lfloor 13\log_2 n\rfloor}{2}} \cdot (1+o(1))$$

distinct labeled graphs G with n vertices and endomorphism monoid isomorphic to M (we denote this fact by End $G \simeq M$). Further there exist

$$\geqslant \frac{(1+o(1))}{\lceil (n-13\log_2 n)\rceil !} \cdot 2^{\binom{n-\lfloor 13\log_2 n\rfloor}{2}}$$

nonisomorphic graphs G with n vertices and End $G \simeq M$ and

$$\geqslant \frac{(1+o(1))}{\lceil (n-13\log_2 n)\rceil !} \cdot \left(\begin{pmatrix} \binom{n-\lfloor 13\log_2 n\rfloor}{2} \\ \left\lfloor \frac{1}{2}\binom{n-\lfloor 13\log_2 n\rfloor}{2} \right\rfloor \end{pmatrix} \right)$$

graphs with n vertices having no homomorphism into each other and End $G \simeq M$.

I. Classes of Rigid Graphs

In this section $\mathfrak{A}_n$ denotes the set of all graphs with n vertices $\{0, 1, 2, \ldots, n-1\}$ and $\lfloor \frac{1}{2}\binom{n}{2} \rfloor$ edges and $\mathfrak{B}_n$ the set of all graphs with n vertices $\{0, 1, \ldots, n-1\}$. For a graph G denote by $E(G)$ the set of all edges of G (i.e., if $G \in \mathfrak{A}_n$ then $G = (\{0, 1, \ldots, n-1\}, E(G))$). For an edge $e \in E(G)$ we shall write also $e \in G$. We shall often use the following lemma, see [5].

Lemma 1.1. *For all positive integers m, k and reals $p, q \geqslant 0$ with $p+q=1$*

$$\sum \binom{m}{t} p^t q^{m-t} \leqslant \exp\left[(m-k)\cdot \ln \frac{mq}{(m-k)} + k \cdot \ln \frac{mp}{k} \right],$$

where the sum is taken over all t such that either $t \geqslant k$ if $k \geqslant pm$ or $t \leqslant k$ if $k \leqslant pm$.

Lemma 1.2. *Let n be a positive integer satisfying $n \geqslant 60 \ln n + 2$. Denote by $f_1(n)$ the number of graphs $G \in \mathfrak{B}_n$ such that there exist two sequences of distinct vertices $\{x_1, x_2, \ldots, x_m\}$, $\{y_1, y_2, \ldots, y_m\}$ such that for at most $\frac{2}{4}\binom{m_n}{2}$ pairs i, j, $1 \leqslant i < j \leqslant m_n$,*

$$\{\{x_i, x_j\}\{x_i, y_j\}, \{y_i, x_j\}, \{y_i, y_j\}\} \cap E(G) \neq \varnothing.$$

(*Here m_n is any number such that $n/2 \geqslant m_n \geqslant 30 \ln n + 1$.*) *Then*

$$f_1(n) \leqslant \left(\frac{1}{n}\right)^{20 \ln n} \cdot 2^{\binom{n}{2}}.$$

Proof. Choose two sequences of distinct vertices $\{x_1, x_2, ..., x_m\}$ $\{y_1, y_2, ..., y_m\}$ in $\{0, 1, ..., n-1\}$. The number of all graphs $G \in \mathfrak{B}_n$ such that there exist at most $\frac{3}{4}\binom{m_n}{2}$ pairs i, j, $1 \leqslant i < j \leqslant m_n$, with $\{\{x_i, x_j\}, \{x_i, y_j\}, \{y_i, x_j\}, \{y_i, y_j\}\} \cap E(G) \neq \varnothing$ is equal to

$$\begin{aligned}
&2^{\binom{n}{2}-4\binom{m_n}{2}} \sum_{j \leqslant (3/4)\binom{m_n}{2}} \left(\binom{\binom{m_n}{2}}{j}\right) \cdot 15^j \\
&= 2^{\binom{n}{2}} \sum_{j \leqslant (3/4)\binom{m_n}{2}} \left(\binom{\binom{m_n}{2}}{j}\right) \cdot \left(\frac{15}{16}\right)^j \left(\frac{1}{16}\right)^{\binom{m_n}{2}-j} \\
&\leqslant 2^{\binom{n}{2}} \exp\left\{\left[\left(1-\frac{3}{4}\right) \ln \frac{1}{16(1-3/4)} + \frac{3}{4} \ln \frac{15}{16(3/4)}\right]\binom{m_n}{2}\right\} \\
&< 2^{\binom{n}{2}} \exp\left(-0{,}179 \binom{m_n}{2}\right).
\end{aligned}$$

Hence the number of graphs fulfilling the conditions of Lemma 1.2 is less than

$$\begin{aligned}
&\sum_{(n/2) \geqslant m_n \geqslant 30 \ln n + 1} \binom{n}{2m_n} \cdot \binom{2m_n}{m_n} \cdot m_n! \cdot \exp\left(-0.179 \binom{m_n}{2}\right) 2^{\binom{n}{2}} \\
&\leqslant \sum_{(n/2) \geqslant m_n \geqslant 30 \ln n + 1} n^{2m_n} \cdot \exp[(-0.179 \cdot 15 \ln n) \cdot m_n] \, 2^{\binom{n}{2}} \\
&\leqslant \sum_{(n/2) \geqslant m_n \geqslant 30 \ln n + 1} \left(\frac{1}{n}\right)^{0.68 m_n} 2^{\binom{n}{2}} \leqslant \left(\frac{1}{n}\right)^{20 \ln n} \cdot 2^{\binom{n}{2}}.
\end{aligned}$$

LEMMA 1.3. *Denote by $f_2(n)$ the number of graphs $G \in \mathfrak{B}_n$ such that for a pair x, y of vertices of G either*

$$|\{z; \{x, z\}, \{y, z\} \in G\}| \geqslant \tfrac{11}{40} n \qquad \text{or} \qquad |\{z; \{x, z\}, \{y, z\} \in G\}| \leqslant \tfrac{9}{40} n.$$

Then there is n_0 such that for $n \geqslant n_0$

$$f_2(n) \leqslant c^{-n} 2^{\binom{n}{2}}, \qquad \text{where} \quad c > 1.$$

Proof. Let x, y be a fixed pair of vertices of $\{0, 1, \ldots, n-1\}$. Then the number of graphs $G \in \mathfrak{B}_n$ with $|\{z; \{x, z\}, \{y, z\} \in G\}| = j$ is

$$2 \cdot \binom{n-2}{j} \cdot 3^{n-j-2} \cdot 2^{\binom{n-2}{2}} < \binom{n}{j} \cdot 3^{n-j} \cdot 2^{\binom{n-2}{2}}$$
$$= 8 \cdot \binom{n}{j} \cdot \left(\frac{3}{4}\right)^{n-j} \cdot \left(\frac{1}{4}\right)^{j} \cdot 2^{\binom{n}{2}}.$$

Thus we get

$$f_2(n) \leqslant \binom{n}{2} \cdot \sum_{|j-(n/4)| \geqslant (n/40)} \binom{n}{j} \cdot \left(\frac{3}{4}\right)^{n-j} \cdot \left(\frac{1}{4}\right)^{j} \cdot 2^{\binom{n}{2}+3}$$
$$\leqslant \binom{n}{2} \cdot (\exp(-0.0016n) + \exp(-0.0017n)) \cdot 2^{\binom{n}{2}+3}$$

and hence $f_2(n) \leqslant c^{-n} \cdot 2^{\binom{n}{2}}$, where $c > 1$.

Analogously, we can prove

LEMMA 1.4. *Denote by $f_3(n)$ the number of graphs $G \in \mathfrak{B}_n$ such that for a vertex x of G either*

$$|\{z; \{x, z\} \in G\}| \geqslant \tfrac{11}{20} n \qquad \text{or} \qquad |\{z; \{x, z\} \in G\}| \leqslant \tfrac{9}{20} n.$$

Then there is n_0 such that for $n > n_0$

$$f_2(n) \leqslant c^{-n} \cdot 2^{\binom{n}{2}}, \qquad \text{where} \quad c > 1.$$

LEMMA 1.5. *Consider a positive integer n satisfying $n \geqslant 30 \ln n + 1$. Denote by $f_4(n)$ the number of graphs $G \in \mathfrak{B}_n$ such that there exists a subgraph of G with m_n vertices and with the number of edges greater than $\frac{3}{4}\binom{m_n}{2}$, where $n \geqslant m_n \geqslant 30 \ln n + 1$. Then*

$$f_4(n) \leqslant \left(\frac{1}{n}\right)^{20 \ln n} \cdot 2^{\binom{n}{2}}.$$

Proof. The number of graphs in $\mathfrak{B}_n$ containing a subgraph of m_n vertices and more than $\frac{3}{4}\binom{m_n}{2}$ edges is at most

$$\binom{n}{m_n} \sum_{j \geqslant \frac{3}{4}\binom{m_n}{2}} \left(\!\binom{\binom{m_n}{2}}{j}\!\right) \cdot 2^{\binom{n}{2}-\binom{m_n}{2}}$$

$$= \binom{n}{m_n} \sum_{j \geqslant \frac{3}{4}\binom{m_n}{2}} \left(\!\binom{\binom{m_n}{2}}{j}\!\right) \cdot \left(\frac{1}{2}\right)^{j} \cdot \left(\frac{1}{2}\right)^{\binom{m_n}{2}-j} 2^{\binom{n}{2}}$$

$$\leqslant n^{m_n} \exp\left(-0.13\binom{m_n}{2}\right) \cdot 2^{\binom{n}{2}} < \left(\frac{1}{n}\right)^{0.96m} \cdot 2^{\binom{n}{2}}.$$

Thus we get

$$f_4(n) \leqslant \sum_{n \geqslant m_n \geqslant 30 \ln n + 1} \left(\frac{1}{n}\right)^{0.96m_n} \cdot 2^{\binom{n}{2}} \leqslant \left(\frac{1}{n}\right)^{20 \ln n} \cdot 2^{\binom{n}{2}}.$$

While the above lemmas are folklore the next lemma is a well-known result of Erdős [7].

LEMMA 1.6. *Let $\varepsilon > 0$. Denote by $f_5(n)$ the number of all graphs $G \in \mathfrak{B}_n$, such that either G or the complement of G contain a complete graph of size greater than $(2 \log_2 n)(1+\varepsilon)$. Then there exists n_ε such that for $n \geqslant n_\varepsilon$*

$$f_5(n) \leqslant \left(\frac{1}{n}\right)^{2\varepsilon \log_2 n} \cdot 2^{\binom{n}{2}}.$$

The following is a result of Erdős and Rényi [8]:

LEMMA 1.7. *Denote by $f_6(n)$ the number of graphs $G \in \mathfrak{B}_n$ with a nontrivial (i.e., nonidentity) automorphism. Then*

$$f_6(n) = \left(\binom{n}{2} \Big/ 2^{n-2}\right) 2^{\binom{n}{2}}(1+o(1)).$$

LEMMA 1.8. *Let $\varepsilon > 0$. There are $t_n = 2^{\binom{n}{2}} \cdot (1+o(1))$ rigid graphs $G_1, G_2, \ldots, G_{t_n} \in \mathfrak{B}_n$ and s_n rigid graphs $H_1, H_2, \ldots, H_{s_n} \in \mathfrak{A}_n$, where*

$$s_n = (1+o(1)) \cdot \left(\!\binom{\binom{n}{2}}{\left\lfloor \frac{1}{2}\binom{n}{2} \right\rfloor}\!\right),$$

such that

(a) *for any pair* i, j, $1 \leqslant i, j \leqslant t_n$ (*or* s_n) *if* $\varphi: G_i \to G_j$ (*or* $\varphi: H_i \to H_j$) *is a homomorphism, then* φ *is a bijection*;

(b) *for any* i, $1 \leqslant i \leqslant t_n$ (*or* $1 \leqslant i \leqslant s_n$) G_i (*or* H_i) *does not contain a complete subgraph with more than* $(2 \log_2 n)(1 + \varepsilon)$ *vertices.*

Proof. We shall prove the existence of G_i $(1 \leqslant i \leqslant t_n)$. The proof of the existence of H_i $(1 \leqslant i \leqslant s_n)$ follows from the fact that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} = 2^n \Big/ \sqrt{\frac{\pi}{2} \cdot n}\,(1 + o(1)),$$

which is a consequence of Stirling formula. Let $f(n)$ be the number of all graphs $G \in \mathfrak{B}_n$ fulfilling either the condition of Lemma 1.2, or the condition of Lemma 1.3, or the condition of Lemma 1.4, or the condition of Lemma 1.5, or the condition of Lemma 1.6 for $\varepsilon' = \min\{\varepsilon, 1\}$, or the condition of Lemma 1.7. Then by the foregoing lemmas there is n_0 such that for $n \geqslant n_0$,

$$f(n) \leqslant c \cdot \left(\frac{1}{n}\right)^{2\varepsilon \log_2 n} \cdot 2^{\binom{n}{2}}, \qquad \text{where} \quad c > 1.$$

Let $G_1, G_2, \ldots, G_{t_n}$ be all the other graphs in $\mathfrak{B}_n$. Then $t_n = 2^{\binom{n}{2}} \cdot (1 + o(1))$ and $G_1, G_2, \ldots, G_{t_n}$ fulfil (b).

We prove (a). If $\varphi: G_i \to G_j$ is a homomorphism which is not one-to-one then there exist vertices x, y of G_i with $\varphi(x) = \varphi(y)$. Then, by the choice of graphs $G_1, G_2, \ldots, G_{t_n}$ we have $|\{z;$ either $\{x, z\} \in G_i$ or $\{y, z\} \in G_i\}| \geqslant 2\frac{9}{20}n - \frac{11}{40}n = \frac{25}{40}n$. By the condition of Lemma 1.6 we obtain that the preimage of any vertex of G_j has size at most $4 \log_2 n$, by the condition of Lemma 1.4 for each vertex t of G_j $|\{z; \{z, t\} \in G_j\}| \leqslant \frac{11}{20}n$ and thus there exist at least $2m$ distinct vertices, $m = 3n/160 \log_2 n$, $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m$, satisfying $\varphi(x_i) = \varphi(y_i)$ for each $i = 1, 2, \ldots, m$. This contradicts the conditions of Lemmas 1.2 and 1.5 because $3n/160 \log_2 n \geqslant 30 \ln n + 1$ for sufficiently large n. Thus φ is one-to-one and hence (as $\{0, 1, \ldots, n-1\}$ is finite) also a bijection. Since every bijective endomorphism of a finite graph is an automorphism we conclude that almost all graphs are rigid.

THEOREM 1.9. *Let* $\varepsilon > 0$. *There are* $((1 + o(1))/n!) \cdot 2^{\binom{n}{2}}$ *pairwise nonisomorphic rigid graphs* $G \in \mathfrak{B}_n$ *such that*

(a) *any homomorphism between an arbitrary pair of them is a bijection*;

(b) *none of these graphs nor its complement contain a complete graph with* $\geqslant (2 \log_2 n)(1 + \varepsilon)$ *vertices.*

Proof. Take graphs $G_1, G_2, \ldots, G_{t_n}$ from Lemma 1.8. As all of them have no nontrivial automorphism for every i, $1 \leqslant i \leqslant t_n$ there are at most $n!$ graphs G_j, $1 \leqslant j \leqslant t_n$, which are isomorphic to G_i. Thus we can find $t_n/n!$ nonisomorphic rigid graphs in $\mathfrak{B}_n$ having properties (a) and (b) of Lemma 1.8.

Note that it is easy to see that there exist at most $(1 + o(1))/n! \cdot 2^{\binom{n}{2}}$ nonisomorphic graphs on a given n point set.

THEOREM 1.10. *Let $\varepsilon > 0$. There are*

$$u_n = \frac{(1 + o(1))}{n!} \cdot \left(\begin{array}{c} \binom{n}{2} \\ \left\lfloor \frac{1}{2}\binom{n}{2} \right\rfloor \end{array} \right)$$

pairwise nonisomorphic graphs $H_1, H_2, \ldots, H_{u_n} \in \mathfrak{U}_n$ such that

(a) *if $\varphi: H_i \to H_j$ is a homomorphism $1 \leqslant i, j \leqslant u_n$ then $i = j$ and φ is the identity;*

(b) *for any i, $1 \leqslant i \leqslant u_n$ neither H_i nor its complement contain a complete subgraph with $\geqslant (2 \log_2 n)(1 + \varepsilon)$ vertices.*

Moreover, if $H_1', H_2', \ldots, H_{v_n}' \in \mathfrak{B}_n$ is a family of graphs satisfying (a) *then*

$$v_n \leqslant \frac{1}{n!} \cdot \left(\begin{array}{c} \binom{n}{2} \\ \left\lfloor \frac{1}{2}\binom{n}{2} \right\rfloor \end{array} \right).$$

Proof. The proof of the first part is analogous to the proof of Theorem 1.9. Condition (a) is obtained from the fact that every bijective homomorphism between graphs with the same number of edges is an isomorphism. We shall prove the final statement: Let $H_1', H_2', \ldots, H_{v_n}' \in \mathfrak{B}_n$ be graphs satisfying (a). This condition ensures clearly that all H_i', $1 \leqslant i \leqslant v_n$, have no nontrivial automorphism. Thus to any H_i', $1 \leqslant i \leqslant v_n$ there exist $n!$ graphs in $\mathfrak{B}_n$ which are isomorphic to H_i' and we get $n!\, v_n$ pairwise distinct graphs. As the edge sets of these graphs form an antichain in the power set of $\{0, 1, \ldots, n-1\}^2$ we get from Sperner's theorem [17 or 15, 13.21] that

$$n!\, v_n = \left(\begin{array}{c} \binom{n}{2} \\ \left\lfloor \frac{1}{2}\binom{n}{2} \right\rfloor \end{array} \right).$$

II. Representation of a General Monoid

First recall that if (X, R) is a k-uniform hypergraph (k-hypergraph), where $k > 1$, then a sequence of the hyperdges $A_1, A_2, \ldots, A_p$ of (X, R) is called a path of length p from x to y ($x, y \in X$) if

(a) $x \in A_1$, $y \in A_p$;

(b) $A_i \cap A_{i+1} \neq \emptyset$ for every $i = 1, 2, \ldots, p-1$.

Similarly, for $n \geqslant k$ the sequence $Z_1, Z_2, \ldots, Z_p$ of subsets of X is called an n-path of length p from x to y if

(a) $x \in Z_1$, $y \in Z_p$;

(b) $|Z_i| = n$ for every $i = 1, 2, \ldots, p$;

(c) $|Z_i \cap Z_{i+1}| = n-1$ for every $i = 1, 2, \ldots, p-1$;

(d) for every $i = 1, 2, \ldots, p$ every k-point subset of Z_i is contained in R.

If (X, R), (X', R') are two hypergraphs then $f: X \to X'$ satisfying $f(A) \in R'$ for every $A \in R$ is called a homomorphism. Note that every homomorphism preserves paths and n-paths.

The proof of the following lemma is based on an idea from [12].

Lemma 2.1. *For every triple of positive integers m, n, k with $m > 6n$, $n \nmid m$ (n does not divide m), $n \geqslant k+1$, $k \geqslant 2$ there exists a k-hypergraph $\mathfrak{T}(m, n, k) = (Z, S)$ with distinct vertices $a, b \in Z$ such that*

(a) *for every pair of distinct vertices $x, y \in Z$ there exists an n-path from x to y;*

(b) *every vertex of Z has degree $\leqslant \binom{n-1}{k-1} + (n-1)\binom{n-2}{k-2}$;*

(c) *every path from a to b has length greater than 3;*

(d) $|Z| = m$;

(e) *$\mathfrak{T}(m, n, k)$ is rigid.*

Proof. Put $Z = \{0, 1, \ldots, m-1\}$, $B = \{1, 2, \ldots, k-1, 2n\}$. Note also that in what follows, addition is taken mod m. Define $S = \{A; \exists p \leqslant m-n, A \in \{p, p+1, \ldots, p+n-1\}, |A| = k\} \cup \{B\}$. Put $\mathfrak{T}(m, n, k) = (Z, S)$. Then clearly, (a), (b), and (d) hold. If we put $a = 0$, $b = 3n$ then (c) holds too, because $m > 6n$. It remains to prove (e). First we show that if $f: (Z, S) \to (Z, S)$ is an endomorphism then f is a bijection. For this reason we show that the strong chromatic number of $\mathfrak{T}(m, n, k)$ is greater than n (by the strong chromatic number of a k-uniform hypergraph (Z, S) we understand the minimal number of colors which are needed to color the set Z in such a way that any $A \in S$ gets k colors). Assume the contrary. Then there exists a partition of $Z = \bigcup_{i=0}^{n-1} Z_i$ such that $|Z_i \cap A| \leqslant 1$ for every

$A \in S$ and $i = 0, 1, \ldots, n-1$. Hence for every $p \leqslant m-n$ and for every $i = 0, 1, \ldots, n-1$, $|Z_i \cap \{p, p+1, \ldots, p+n-1\}| = 1$. Thus we get if $0 \in Z_i$ then $n, 2n, \ldots, \lfloor m/n \rfloor \cdot n \in Z_i$. Moreover for each $j = 0, 1, \ldots, n-1$ with $j + \lfloor m/n \rfloor \cdot n \leqslant m$ if $j \in Z_i$ then $j+n$, $j+2n, \ldots, j + \lfloor m/n \rfloor \cdot n \in Z_i$. Since $0 \equiv m \pmod m$ we get that 0 and $m - \lfloor m/n \rfloor n$ are in the same set Z_i; this is a contradiction because $0 < m - \lfloor m/n \rfloor \cdot n \leqslant n-1$ (as $n \nmid m$). On the other hand for every $0 \leqslant i < j \leqslant m-1$, $|j-i| < m$, we have that the subgraph on the set $\{i+p;\ p = 0, 1, \ldots, j-i\}$ has strong chromatic number $\leqslant n$ (put $Z_k = \{i+p;\ p \equiv k \pmod n\}$ for each $k = 0, 1, \ldots, n-1$, then $\{Z_k; k = 0, 1, \ldots, n-1\}$ is the required partition).

Let $i \in \{1, 2, \ldots, m-2\}$, then for any pair j, k, $0 \leqslant j < i < k \leqslant m-1$, each n-path from j to k contains i; therefore, by (a), if $f: (Z, S) \to (Z, S)$ is an endomorphism and $i \notin \operatorname{Im} f$ then either $\operatorname{Im} f \subset \{0, 1, \ldots, i-1\}$, or $\operatorname{Im} f \subset \{i+1, i+2, \ldots, m-1\}$ but this is impossible. Thus f is surjective and because Z is finite we have that f is a bijection and automorphism of (Z, S). Thus x and $f(x)$ are contained in the same number of n-cliques (n point subsets of Z every k element subset of which is an element of R). Hence $f(\{0, 1, m-1\}) = \{0, 1, m-1\}$. Therefore $f(0) = 0$ and if we consider that $f(B) = B$ we get $f(1) = 1$, $f(m-1) = m-1$. Now we can prove by induction that f is the identity.

DEFINITION. Let (V, U) be a graph and $\{V_i; i \in I\}$ a partition of V, let $i_0 \in I$. We say that the family $\{(V, U), \{V_i; i \in I\}, i_0\}$ is *nice* if

(i) for every edge $\{x, y\} \in U$ and $i \in I$, $x \in V_i$ implies $y \notin V_i$;

(ii) for every $i \in I - \{i_0\}$ and every $v \in V_i$ there exists $u \in V_{i_0}$ with $\{v, u\} \in U$;

(iii) there exists $j \in I$ such that for each $v \in V_{i_0}$ there is $u \in V_j$ with $\{v, u\} \in U$;

(iv) for every $v \in V_i$, $i \neq i_0$ there exists $u \in V - V_{i_0}$ with $\{v, u\} \in U$.

CONSTRUCTION 2.2. Let $\kappa = \{(V, U), \{V_i; i \in I\}, i_0\}$ be a nice family. Let $G = (Y, T)$ be a graph (possibly empty) and n a positive integer, $n \geqslant 3$. Choose the smallest number m with $n \nmid m$, $m > 6n$, $m \geqslant |I| + 2n - 1$. Choose $j \in I$ such that for every $u \in V_{i_0}$ there is $v \in V_j$ with $\{u, v\} \in U$ (such j exists, as κ is nice). Put $(Z, S) = \mathfrak{T}(m, n, 2)$ and choose $a, b, c \in Z$ such that every path from a to b has length greater than 3 and $\{a, c\} \notin S$. Choose a one-to-one mapping $\mu: I \to Z$ fulfilling:

(a) $\mu(i_0) = a$, $\mu(j) = b$,

(b) if $\{a, x\} \in S$ then $x \notin \mu(I)$,

(c) $c \notin \mu(I)$.

Assume that V, Y, Z are disjoint sets and put $X = V \cup Y \cup Z$. Choose $y_0 \in Y$ (if Y is nonempty) and define $R = U \cup T \cup S \cup \{\{x, y\};\ \exists i \in I,\ x \in V_i,\quad y = \mu(i)\} \cup \{\{y, c\};\quad y \in Y\} \cup \{\{v, y_0\};\quad v \in V_{i_0}\}$. Then put $C(\kappa, G, n, \mu, c, y_0) = (X, R)$.

LEMMA 2.3. *Let $\kappa^j = \{(V^j, U^j), \{V_i^j;\ i \in I^j\}, i_0^j\}$, $j = 1, 2$, be nice families with $|I^1| = |I^2|$. Let $G^j = (Y^j, T^j)$, $j = 1, 2$, be connected graphs. Let n be a positive integer greater than the size of the largest clique in any of the graphs (V^j, U^j) and G^j, $j = 1, 2$. Then $f: C(\kappa^1, G^1, n, \mu^1, c^1, y^1) \to C(\kappa^2, G^2, n, \mu^2, c^2, y^2)$ is a homomorphism iff the following conditions hold:*

(i) $c^1 = c^2$,

(ii) $f(Y^1) \subset Y^2$ *and* f/Y^1 *is a homomorphism from* G^1 *to* G^2 *satisfying* $f(y^1) = y^2$;

(iii) $f(V^1) \subset V^2$ *and* f/V^1 *is a homomorphism from* (V^1, U^1) *to* (V^2, U^2);

(iv) *there exists a bijection* $v: I^1 \to I^2$ *such that* $\mu_1 = \mu_2 \circ v$, $v(i_0^1) = i_0^2$ *and* $f(V_i^1) \subset V_{(i)}^2$ *for each* $i \in I^1$;

(v) $f(x) = x$ *for every* x *which is not an element of either* Y^1 *or* V^1.

Proof. Assume that $f: C(\kappa^1, G^1, n, \mu^1, c^1, y^1) \to C(\kappa^2, G^2, n, \mu^2, c^2, y^2)$ is a homomorphism. If $(X^1, R^1) = C(\kappa^1, G^1, n, \mu^1, c^1, y^1)$ and $(X^2, R^2) = C(\kappa^2, G^2, n, \mu^2, c^2, y^2)$ then $X^1 = V^1 \cup Y^1 \cup Z$, $X^2 = V^2 \cup Y^2 \cup Z$ because $|I^1| = |I^2|$ and $\mathfrak{T}(m, n, 2) = (Z, S)$, where m is the smallest positive integer with $n \nmid m$, $m > 6n$ and $m \geqslant |I^1| + 2n - 1$. Since every pair of vertices z_1, z_2 of Z is contained in an n-path and since n is greater than the size of the largest clique in any of the graphs (V^j, U^j) and G^j $(j = 1, 2)$ we see that $f(Z) \subset Z$ and so by (e) in Lemma 2.1, $f(z) = z$ for every $z \in Z$. Thus (v) holds.

Now we show that $f(V_{i_0^1}^1) \cap Z = \emptyset$. If $v \in V_{i_0^1}^1$ then there exists $u \in V_j^1$ (by (iii) in the definition of a nice family) with $\{u, v\} \in U^1$, where $\mu^1(j) = b$. Then $\{a, v\}$, $\{v, u\}$, $\{u, b\} \in R^1$. Thus we have $\{a, f(v)\}$, $\{f(v), f(u)\}$, $\{f(u), b\} \in R^2$ and hence also $f(v) \notin Z$ (as $f(v) \in Z$ implies $f(u) \in Z$ and this contradicts the fact that every path in (Z, S) from a to b has length greater than 3). Therefore $f(v) \in V_{i_0^2}^2$ (we use the property of μ^2 that $\mu(i_0^2) = a$; see (a) in Construction 2.2) and thus $f(V_{i_0^1}^1) \subset V_{i_0^2}^2$.

If $v \in V_i^1$ for some $i \in I^1$ then $\{v, \mu^1(i)\} \in R^1$ and $\{v, u\} \in U^1 \subset R^1$ for some $u \in V_{i_0^1}^1$. Thus $\{f(u), f(v)\}$, $\{f(v), \mu^1(i)\} \in R^2$. Since $f(u) \in V_{i_0^2}^2$ we get by (b) in Construction 2.2 that $f(v) \notin Z$ ($\{a, \mu^1(i)\} \notin S$). Hence $f(v) \in V^2$ or $f(v) \in Y^2$. If $f(v) \in Y^2$ then $c^2 = \mu^1(i)$. By (iv) in the definition of a nice family there exists $w \notin V_{i_0^1}^1$ such that $\{v, w\} \in U^1$ and $w \in V_j^1$, $j \neq i$. Then $f(w) \in V_k^2$ for some $k \in I^2$ with $\mu^1(j) = \mu^2(k)$. Now $\{f(v), f(w)\} \in R^2$ and because $k \neq i_0^2$ we get $f(v) \notin Y^2$. Thus there exists $i^* \in I^2$ with $f(v) \in V_{i^*}^2$.

Put $\nu(i) = i^*$. Then $\mu^1 = \mu^2 \cdot \nu$ and $f(v) \in V^2_{\nu(i)}$ if $v \in V^1_i$. Since $\nu(i^1_0) = i^2_0$ we find that (iv) holds and (iii) is a consequence of (iv).

Now we prove (i) and (ii). Since $\{y^1, c^1\}, \{y^1, v\} \in R^1$ for each $v \in V^1_{i^1_0}$ we have $\{c^1, f(y^1)\}, \{f(y^1), f(v)\} \in R^2$. As $f(v) \in V^2_{i^2_0}$ and $\{c^1, a\} \notin S^0$ we obtain $f(y^1) \notin Z$. Since $|I^1| = |I^2|$ it follows from (iv) and (v) $f(y^1) \notin V^2$—thus $f(y^1) \in Y^2$ and moreover $f(y^1) = y^2$. Hence $c^1 = c^2$ and by connectedness of G^1 we get $f(Y^1) \subset Y^2$. Thus (i) and (ii) hold, also. It is a matter of routine to verify that if f fulfils (i)–(v) then f is also a homomorphism. Therefore we omit the proof.

CONSTRUCTION 2.4. Let $\mathcal{M} = (M, \cdot, 1)$ be a monoid with a set N of generators. Put $k = \lceil (1 + \sqrt{1 + 8|N|})/2 \rceil + 1$ and $I = \{0, 1, \ldots, k-1\}$. Choose a one-to-one mapping ν from N to the set of all two-point subsets of $I - \{0\}$ (by the choice of k this is possible). Define $V = M \times I$,

$$U = \{\{(x, 0), (x, i)\}; x \in M, i \in I - \{0\}\} \cup \{\{(x, i), (gx, j)\}; g \in N, \nu(g) = \{i, j\}, i < j, x \in M\}.$$

Set $V_i = M \times \{i\}$ for $i \in I$. Then the family $\mathcal{G}(\mathcal{M}, N) = \{(V, U), \{V_i; i \in I\}, 0\}$ is nice.

LEMMA 2.5. *Let $\mathcal{M} = (M, \cdot, 1)$ be a monoid with set N of generators. If $\mathcal{G}(\mathcal{M}, N) = \{(V, U), \{V_i; i \in I\}, 0\}$ then $\varphi: V \to V$ with $\varphi(V_i) \subset V_i$ for each $i \in I$ is a homomorphism of (V, U) into itself iff $\varphi = \psi \times 1_I$, where ψ is a right translation of $\mathcal{M}$ and 1_I is the identity mapping of I.*

Proof. Assume that $\varphi: V \to V$ is an endomorphism of (V, U) and $\varphi(V_i) \subset V$ for each $i \in I$. Since $\varphi(V_0) \subset V_0$ there is $\psi: M \to M$ with $\varphi(x, 0) = (\psi(x), 0)$ for $x \in M$ $(V_0 = M \times \{0\})$. For each $x \in M$ and $i \in I - \{0\}$, $\{(x, 0), (x, i)\} \in U$. Thus $\{\varphi(x, 0) = (\psi(x), 0), \varphi(x, i)\} \in U$, but $\varphi(x, i) = (y, i)$ because $\varphi(V_i) \subset V_i$—and so $\varphi = \psi \times 1_I$. Further for each $g \in N$, if $\nu(g) = \{i, j\}$, $i < j$, then for each $x \in M$, $\{(x, i), (gx, j)\} \in U$—thus $(\psi(x), i), (\psi(gx), j)\} \in U$ and so $\psi(gx) = g\psi(x)$. Thus this equality holds for each $x \in M$ and so ψ commutes with left translation by g. Because $g \in N$ is arbitrary we get that ψ commutes with any left translation of $\mathcal{M}$ hence ψ is a right translation of $\mathcal{M}$ (see [6, Chap. 1). Conversely, if $\varphi = \psi \times 1_I$ where ψ is a right translation then ψ commutes with any left translation of $\mathcal{M}$; thus $\{\varphi(x, i) = (\psi(x), i), \varphi(gx, j) = (\psi(gx), j) = (g\psi(x), j)\} \in U$ for any $g \in N$, $x \in M$ and $i < j$ with $\{i, j\} = \nu(g)$. Further U contains $\{\varphi(x, 0) = (\psi(x), 0), \varphi(x, i) = (\psi(x), i)\}$ for any $x \in M$ and $i \in I - \{0\}$. Therefore φ is a homomorphism.

COROLLARY 2.6. *Let $\mathcal{M}$ be a monoid with a set N of generators, let G*

be a rigid graph and let n be a positive integer greater than the size of any complete subgraph of G and $n > \lceil (1 + \sqrt{1 + 8|N|})/2 \rceil + 1$. *Then for every* μ, c, y *the endomorphism monoid of* $C(\mathcal{G}(\mathcal{M}, N), G, n, \mu, c, y)$ *is isomorphic to* $\mathcal{M}$.

Proof. If a family $\{(V, U), \{V_i; i \in I\}, i_0\}$ is nice then every complete subgraph of (V, U) has size less than or equal to $|I|$. It follows from Lemmas 2.3 and 2.5 that the endomorphism monoid of $C(\mathcal{G}(\mathcal{M}, N), G, n, \mu, c, y)$ is isomorphic to a monoid of all right translations of $\mathcal{M}$ and so also isomorphic to $\mathcal{M}$.

THEOREM 2.7. $M(n) \leqslant O(n^{3/2})$, *more precisely for a monoid* $\mathcal{M} = (M, \cdot, 1)$ *there exists a graph G with at most* $\sqrt{2 \cdot |M|} \cdot (|M| + 6)$ *vertices such that the endomorphism monoid of G is isomorphic to* $\mathcal{M}$.

Proof. In Corollary 2.6 set $G =$ null graph and $N = M$, then we obtain our theorem.

DEFINITION. Let $\mathcal{M}$ be a monoid. Define the functions $\varphi_{\mathcal{M}}$, $\psi_{\mathcal{M}}$ and $\chi_{\mathcal{M}}$ as follows:

$\varphi_{\mathcal{M}}(n)$ is the number of all graphs in $\mathfrak{B}_n$ (with the set of vertices $\{0, 1, \ldots, n-1\}$) such that their endomorphism monoid is isomorphic to $\mathcal{M}$.

$\psi_{\mathcal{M}}(n)$ is the largest positive integer k such that there are k pairwise nonisomorphic graphs in $\mathfrak{B}_n$ with endomorphism monoid isomorphic to $\mathcal{M}$.

$\chi_{\mathcal{M}}(n)$ is the largest positive integer k such that there are k graphs $H_1, H_2, \ldots, H_k$ in $\mathfrak{B}_n$ with

(a) the endomorphism monoid of H_i, $1 \leqslant i \leqslant k$ is isomorphic to $\mathcal{M}$,

(b) if $\varphi: H_i \to H_j$ is a homomorphism, $1 \leqslant i, j \leqslant k$ then $i = j$.

THEOREM 2.8. *If n is large enough then for every monoid and* $\varepsilon > 0$,

$$\varphi_{\mathcal{M}}(n) \geqslant 2^s, \qquad \psi_{\mathcal{M}}(n) \geqslant \frac{1}{\lceil t \rceil!} \cdot 2^s, \qquad \text{and} \qquad \chi_{\mathcal{M}}(n) \geqslant \frac{1}{\lceil t \rceil!} \cdot \binom{s}{\lfloor \frac{s}{2} \rfloor},$$

where $t = (n - (12 + \varepsilon) \log_2 n$ *and* $s = \binom{\lceil t \rceil}{2}$.

Proof. If $\mathcal{M} = (M\cdot, 1)$ take n with $\log_2 n \geqslant \sqrt{2 \cdot |M|} \cdot (|M| + 6)$. Put $t_n = n - (12 + \varepsilon) \cdot \log_2 n - (\sqrt{2 \cdot |M|}^3)$. It follows by Lemma 1.8, Theorems 1.9 and 1.10 that there are three families of distinct rigid graphs $\{H_1, H_2, \ldots, H_{u_n}\}$, $\{G_1, G_2, \ldots, G_{v_n}\}$, $\{F_1, F_2, \ldots, F_{w_n}\} \subset \mathfrak{B}_n$ such that

(a) $u_n = 2^{\binom{t_n}{2}} \cdot (1 + o(1))$, $v_n = 2^{\binom{t_n}{2}} \cdot (1 + o(1))/t_n!$, and

$$w_n = \binom{\binom{t_n}{2}}{\left\lfloor \frac{1}{2}\binom{t_n}{2} \right\rfloor} \frac{1 + o(1)}{t_n!};$$

(b) if $1 \leqslant j, i \leqslant v_n$ then G_i, G_j are nonisomorphic;

(c) if $1 \leqslant j, i \leqslant w_n$ and $\varphi: F_i \to F_j$ is a homomorphism then $i = j$;

(d) if a complete graph with p vertices is a subgraph of one of those graphs then $p < \lfloor 2 \log_2 n(1 + \varepsilon) \rfloor$ for sufficiently large n. By Lemma 2.3 and Corollary 2.6 we get $\varphi_{\mathcal{M}}(n) \geqslant u_n$, $\psi_{\mathcal{M}}(n) \geqslant v_n$, and $\chi_{\mathcal{M}}(n) \geqslant w_n$.

III. Representation of 3-Nilpotent Monoids

First we give a technical lemma which is useful for a construction of a graph with a given endomorphism monoid. For this purpose we introduce some notation.

We say that a monoid $\mathcal{M}$ is a *subdirect product* of monoids $\mathcal{M}_i$; $i \in I$ if there exists a one-to-one homomorphism $\varphi: \mathcal{M} \to \prod_{i \in I} \mathcal{M}_i$ such that $\varphi \circ \pi_j$ is onto for every projection $\pi_j: \prod_{i \in I} \mathcal{M}_i \to \mathcal{M}_j$.

Definition. We say that a graph (X, R) has a *core* if there exists a subset $Y \subset X$, $|Y| > 1$ such that for every pair x, y of distinct points of Y there exists a 3-path from x to y in (X, R) and for each $x \in X$ there exists $z \in Y$ with $\{x, z\} \in R$. We say that a graph (X, R) is a *canonical representation* of a monoid $\mathcal{M} = (M, \cdot, 1)$ if the endomorphism monoid of (X, R) is isomorphic to $\mathcal{M}$ and there exists a subset Z of X such that

(a) Z is stable, i.e., if $x, y \in Z$ then $\{x, y\} \notin R$;

(b) if f is an endomorphism of (X, R) then $f(Z) \subset Z$;

(c) there exists a bijection $\varphi: M \to Z$ such that for every right translation ψ of $\mathcal{M}$, $\varphi \cdot \psi \cdot \varphi^{-1}$ has a unique extension to an endomorphism of (X, R). Then Z is called a *canonical set* w.r.t. $\mathcal{M}$.

Note. It is clear that each representation constructed in the second section has a core and is canonical.

Proposition 3.1. *Let $\mathcal{M} = (M, \cdot, 1)$ be a subdirect product of monoids $\mathcal{M}_i$; $i \in I$. Assume that there is a family of graphs $\{(X_i, R_i); i \in I\}$ such that*

(i) *(X_i, R_i) has a core for every $i \in I$;*

(ii) *(X_i, R_i) is a canonical representation of $\mathcal{M}_i$ for every $i \in I$;*

(iii) *there is no homomorphism $\varphi: (X_i, R_i) \to (X_j, R_j)$ if $i \neq j$. Then there exists a graph (X, R) which is a canonical representation of the monoid $\mathcal{M}$ such that $|X| = |M| + \sum_{i \in I} |X_i|$.*

Proof. Without loss of generality assume that the sets X_i, $i \in I$, are pairwise disjoint. Moreover, we can assume for every $i \in I$ that $M_i \subset X_i$ and M_i is a canonical set. Then every right translation of $\mathcal{M}_i$ can be extended to a homomorphism of (X_i, R_i). Assume that M is disjoint from $\bigcup_{i \in I} X_i$ and define

$$X = M \cup \bigcup_{i \in I} X_i, \qquad R = \bigcup_{i \in I} R_i \cup \{\{x, \pi_i(x)\}; x \in M. i \in I\},$$

where we assume that $\mathcal{M}$ is a submonoid of $\prod_{i \in I} \mathcal{M}_i$ and $\pi_j: \prod_{i \in I} \mathcal{M}_i \to \mathcal{M}_j$ is the jth projection. Since $\mathcal{M}$ is a subdirect product of $\mathcal{M}_i$, $i \in I$ we can assume that $\mathcal{M}$ is a submonoid of $\prod_{i \in I} \mathcal{M}_i$ such that the restriction of each projection is onto. We shall prove that $\varphi: X \to X$ is an endomorphism of (X, R) iff

(a) $\varphi(M) \subset M$ and the restriction φ on M is a right translation of $\mathcal{M}$;

(b) $\varphi(X_i) \subset X_i$ and φ/X_i is an endomorphism of (X_i, R_i) for every $i \in I$;

(c) if φ/M is a right translation by $m \in M$ in $\mathcal{M}$, then φ/M_i is a right translation by $\pi^i(m)$ in $\mathcal{M}_i$ for every $i \in I$. Then we get that every right translation of $\mathcal{M}$ has a unique extension to an endomorphism of (X, R). Therefore the endomorphism monoid of (X, R) is isomorphic to the monoid of all right translations of $\mathcal{M}$ and thus it is isomorphic to $\mathcal{M}$.

Now we prove that the conditions (a), (b), and (c) are necessary. For each $i \in I$ choose $Z_i \subset X_i$ such that

(1) for each pair $u, v \in Z_i$ there exists a 3-path between u and v;

(2) for each $x \in X_i$ there exists $z \in Z_i$ with $\{x, z\} \in R_i$;

(3) $|Z_i| \geqslant 3$.

The existence of such a set Z_i follows from the fact that (X_i, R_i) has a core. Thus for each $i \in I$ there exists $i_j \in I$ with $\varphi(Z_i) \subset X_{i_j}$ (because $\varphi(Z_i)$ has property (1) as well and there is no triangle containing a point of M). Then by (2) we have $\varphi(X_i) \subset X_{i_j} \cup M$. Since for each $m \in M$ and $i \in I$ there exists exactly one $x \in X_i$ with $\{m, x\} \in R$ we obtain that if $\psi: X_i \cup M \to X_i$ satisfies

(d) $\psi(x) = x$ for $x \in X_i$,

(e) for every $m \in M$ there exists $m_x \in X_i$ with both $\{m, m_x\} \in R$ and $\{m_x, \psi(x)\} \in R_i$;

then it is a homomorphism from the subgraph of (X, R) induced on $M \cup X_i$ to (X_i, R_i). (Note that the existence of a ψ follows from the fact that (X_i, R_i) has no isolated points). Therefore there exists a homomorphism from (X_i, R_i) to (X_{i_j}, R_{i_j}) and hence by assumption (iii) we have that $i = i_j$ for each $i \in I$. Now we prove that $\varphi(X_i) \subset X_i$. We know already that $\varphi(X_i) \subset X_i \cup M$. Assume that $\varphi(x) \in M$ for some $x \in X_i$. We prove:

(A) $x \notin Z_i$—Indeed, if $x \in Z_i$ then there exist $u, v \in Z_i$ with $\{x, u\}$, $\{x, v\}$, $\{u, v\} \in R_i$ and moreover there exists exactly one $z \in Z_i$ with $\{\varphi(x), z\} \in R$. Thus $\varphi(u) = \varphi(v) = z$; a contradiction.

(B) $x \in M_i$. There exists $z \in Z_i$ with $\{x, z\} \in R_i$ and thus also $\{\varphi(x), \varphi(z)\} \in R$. Further there exist $u, v \in Z_i$ with $\{z, u\}$, $\{z, v\}$, $\{u, v\} \in R$ and thus $\{\varphi(z), \varphi(u)\}$, $\{\varphi(z), \varphi(v)\}$, $\{\varphi(u), \varphi(v)\} \in R$. Therefore $\varphi(u) \neq \varphi(v)$. Hence there exist two mappings η, ν fulfilling (d) and (e) and moreover

(f) $\varphi(u) = \eta(\varphi(x)) \neq \nu(\varphi(x)) = \varphi(v)$;

(g) $\eta(y) = \nu(y)$ for each $y \in M \cup X_i$, $y \neq \varphi(x)$.

Then $\eta \cdot \varphi/X_i$, $\nu \cdot \varphi/X_i$ are different endomorphisms of (X_i, R_i) such that $\eta \cdot \varphi(y) = \nu \cdot \varphi(y)$ for each $y \in X_i$, $y \neq x$. As M_i is canonical we get (from (c) of the definition of a canonical set) that $x \in M_i$. Further (from (b) in this definition) we have $\eta \cdot \varphi(x)$, $\nu \cdot \varphi(x) \in M_i$. To finish the proof of the fact that $\varphi(X_i) \subset X_i$ we have $\{\varphi(u) = \eta \cdot \varphi(x), \varphi(v) = \nu \cdot \varphi(x)\} \in R$—this contradicts (a) in the definition of the canonical set. Thus for each $i \in I$, $\varphi(X_i) \subset X_i$. Hence $\varphi(M) \subset M$ and moreover for each $i \in I$, φ/M_i is a right translation of $\mathcal{M}_i$.

Let φ/M_i be the right translation by x_i. Let $x = \{x_i\}_{i \in I} \in \prod_{i \in I} \mathcal{M}_i$. We prove that $x \in M$ and φ/M is a right translation of x. Denote by 1 the identity of $\mathcal{M}$, 1_i the identity of $\mathcal{M}_i$. Then $\{1, 1_i\} \in R$ for each $i \in I$ and $\varphi(1_i) = x_i$. Thus $\{\varphi(1), x_i\} \in R$ for each $i \in I$ this means that $\pi_i(\varphi(1)) = x_i$ and so $\varphi(1) = x$. For $y \in M$ we must prove that $\varphi(y) = yx$. We have $\{y, \pi_i(y)\} \in R$ for each $i \in I$ and $\varphi(\pi_i(y)) = \pi_i(y)x_i$. Then $\{\varphi(y), \pi_i(y)x_i\} \in R$; this means $\pi_i(\varphi(y)) = \pi_i(y)x_i = \pi_i(y)\,\pi_i(x) = \pi_i(yx)$ for each $i \in I$. Hence $\varphi(y) = yx$ and the proofs of (a), (b), and (c) are complete. Let $\varphi; X \to X$ fulfil (a), (b), and (c). Then for each $\{x, y\} \in R$ such that $\{x, y\} \in R_i$ we have $\{\varphi(x), \varphi(y)\} \in R_i \subset R$. We prove that for each $m \in M$, $i \in I$, $\{\varphi(m), \varphi(\pi_i(m))\} \in R$. By (a) there exists $x \in M$ such that φ/M is the right translation of x, i.e., $\varphi(m) = mx$. Further by (c) $\varphi(\pi_i(m)) = \pi_i(m)\,\pi_i(x) = \pi_i(mx)$ and thus $\{\varphi(m), \varphi(\pi_i(m))\} \in R$ and the proof is complete.

In this part we shall investigate a special class of monoids.

DEFINITION. Let G be a groupid with unity 1 and zero 0. We say that G

is 3-nilpotent if for every triple x, y, z of elements of G with $x \neq 1$, $y \neq 1$, $z \neq 1$ we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z = 0$.

The following is clear.

LEMMA 3.2. *Every 3-nilpotent groupoid is a monoid.*

The proof of the following result will be published in [14]. The analogous result for semigroups was proved in [13].

PROPOSITION 3.3. *If $\mathcal{M}(m)$ is the number of monoids on the set $\{0, 1, \ldots, m-1\}$ and $\mathcal{N}(m)$ is the number of 3-nilpotent monoids on the set $\{0, 1, \ldots, m-1\}$ then $\mathcal{M}(m) = (1 + o(1)) \cdot \mathcal{N}(m)$.*

We show now that $\sqrt{2}n(1 + o(1)) \sqrt{\log_2 n} \leqslant N(n) \leqslant 12n \log_2 n + n$. First we describe the algebraic structure of 3-nilpotent monoids. For a 3-nilpotent monoid $\mathcal{M} = (M, \cdot, 1)$ denote by $\eta(\mathcal{M}) = \{x \in X - \{1\};\ \exists y \in X - \{1\},\ xy \neq 0 \text{ or } yx \neq 0\}$, $\nu(\mathcal{M}) = \{x \in X;\ \exists y, z \in X - \{1\},\ x = yz\}$. Then $\eta(\mathcal{M}) \cap \nu(\mathcal{M}) = \varnothing$ and moreover if $x \in X - \eta(\mathcal{M})$, $x \neq 1$ and $y \in X - \{1\}$ then $xy = yx = 0$. Thus each 3-nilpotent monoid is determined by a mapping $\varphi(\mathcal{M})$ from $\eta(\mathcal{M}) \times \eta(\mathcal{M})$ onto $\nu(\mathcal{M})$ (or into $X - \eta(\mathcal{M})$) defined by $\varphi(\mathcal{M})(x, y) = xy$. On the other hand if A, B are subsets of X with $1 \in A, B$, $A \cap B = \varnothing$ and $0 \in B$ then every mapping from $A \times A$ to B uniquely determines a 3-nilpotent monoid.

THEOREM 3.4. $N(n) \geqslant (1 + o(1)) \sqrt{2} \cdot (n \sqrt{\log_2 n})$.

Proof. Let $A \subset X$ be such that $|X - A| \geqslant 3$ and $|X| = n$. Then the number of 3-nilpotent monoids $\mathcal{M}$ on X with $A = \eta(\mathcal{M})$ is $(n - t - 1)^{t^2}$ where $t = |A|$. Thus if $|A| = (n \log_2 n - n)/\log_2 n - 1$ then this number equals

$$2^{(n^2 \log_2 n) \cdot (1 + o(1))}.$$

Hence the number of non-isomorphic 3-nilpotent monoids $\mathcal{M}$ on the n element set X is greater than

$$\frac{1}{n!} 2^{(n^2 \log_2 n) \cdot (1 + o(1))} = 2^{(n^2 \log_2 n) \cdot (1 + o(1))}.$$

Since the number of all nonisomorphic graphs with at most n vertices is less than

$$\sum_{j \leqslant n} 2^{\binom{j}{2}} \leqslant 2^{\binom{n}{2} \cdot (1 + o(1))}$$

we have

$$2^{\binom{N(n)}{2} \cdot (1 + o(1))} \geqslant 2^{(n^2 \log_2 n) \cdot (1 + o(1))}$$

and thus

$$\binom{N(n)}{2} \geqslant (n^2 \log_2 n) \cdot (1 + o(1)).$$

From this, the stated inequality is immediate.

COROLLARY 3.5. $M(n) \geqslant \sqrt{2}(1 + o(1))n \sqrt{\log_2 n}$.

Corollary 3.5 gives a negative answer to the problem (formulated by Babai and Nešetřil) whether there exists a constant c with $M(n) \leqslant cn$.

Now we give an upper bound on $N(n)$.

CONSTRUCTION 3.6. Let $\mathcal{M} = (M, \cdot, 1)$ be a 3-nilpotent monoid with $|v(\mathcal{M})| = 2$. Let $v(\mathcal{M}) = \{a, 0\}$ and let 1 be the identity of $\mathcal{M}$. Put $V = \{(x, y); x, y \in M,\ y \neq 1$ and either $y = x$ or $y \in v(\mathcal{M})$ or $x \in v(\mathcal{M})\}$. Define $U = \{\{(x, 0), (x, y)\};\ x \in M,\ (x, y) \in V\} \cup \{\{(x, a), (zx, z)\};\ x \in M,\ z \in \eta(\mathcal{M})\}$. By the properties of 3-nilpotent monoids we get that $zx \in \{z, a, 0\}$ and thus the definition of U is correct. Define $V_y = \{(x, y);\ \exists x \in M,\ (x, y) \in V\}$ $y \in M - \{1\}$ and put $\varphi(\mathcal{M}) = \{(V, U),\ \{V_y;\ y \in M - \{1\}\}, 0\}$. Clearly, $\varphi(\mathcal{M})$ is a nice family and $|V| = 5|M| - 9$.

LEMMA 3.7. *Let $\mathcal{M} = (M, \cdot, 1)$ be a 3-nilpotent monoid with $|v(\mathcal{M})| = 2$. Let $\varphi(\mathcal{M}) = \{(V, U),\ \{V_y;\ y \in M - \{1\}\}, 0\}$ be as in Construction 3.6. Then a mapping $\varphi: V \to V$ satisfying $\varphi(V_y) \subset V_y$ for every $y \in M - \{1\}$ is a homomorphism iff there exists a right transition ψ of $\mathcal{M}$ such that $\varphi(x, y) = (\psi(x), y)$ for each $(x, y) \in V$.*

The proof is analogous to that of Lemma 2.6 and therefore we omit it.

PROPOSITION 3.8. *Let $\mathcal{M} = (M, \cdot, 1)$ be a 3-nilpotent monoid with $|v(\mathcal{M})| = 2$. Let G be a rigid graph with vertex set of cardinality less than $|M|$. Then for arbitrary μ, y, c $C(\varphi(\mathcal{M}), G, |M|, \mu, c, y)$ has a core and it is a canonical representation of $\mathcal{M}$. Moreover the cardinality of the vertex set of $C(\varphi(\mathcal{M}), G, |M|, \mu, c, y)$ is less than $12|M|$.*

Proof. Let $\varphi(\mathcal{M}) = \{(V, U),\ \{V_y; y \in M - \{1\}\}, 0\}$, $G = (Y, S)$, $\mathfrak{T}(6 \cdot |M| + 1, |M|, 2) = (Z, T)$. Then Z is a core of $C(\varphi(\mathcal{M}), G, M, \mu, c, y)$. It follows by Lemma 2.3 that if φ is an endomorphism of $C(\varphi(\mathcal{M}), G, |M|, \mu, c, y)$ then $\varphi(V_y) \subset V_y$ for each $y \in M - \{1\}$. Then Lemma 3.7 implies that φ/V_0 is a right translation of $\mathcal{M}$. Lemmas 2.3 and 3.7 assert that every right translation has a unique extension to an endomorphism of $C(\varphi(\mathcal{M}), G, |M|, \mu, c, y)$ (we identify V_0 with M, $(x, 0) \sim x$). Thus $C(\varphi(\mathcal{M}), G, |M|, \mu, c, y)$ is a canonical representation of

$\mathcal{M}$. Since $|V| = 5 \cdot |M| - 9$, $|Y| < |M|$, $|Z| = 6 \cdot |M| + 1$, we see that the size of the vertex set of $C(\varphi(\mathcal{M}), G, |M|, \mu, y)$ is less than $5 \cdot |M| - 9 + |M| + 6 \cdot |M| + 1 = 12 \cdot |M| - 8 < 12 \cdot |M|$.

LEMMA 3.9. *For every 3-nilpotent monoid $\mathcal{M} = (M, \cdot, 1)$ there exists a family of 3-nilpotent monoids $\mathcal{M}_i = (M_i, \cdot, 1_i)$, $i \in I$, such that*

(a) *$\mathcal{M}$ is a subdirect product of $\mathcal{M}_i$, $i \in I$;*

(b) $|I| < \log_2(|v(\mathcal{M})| + 1)$;

(c) $|v(\mathcal{M}_i)| = 2$ *for each* $i \in I$;

(d) $|M_i| = |M_j|$ *for all* $i, j \in I$.

Proof. Choose a family $\{B_i; i \in I\}$ of proper subsets of $v(\mathcal{M})$ such that

(i) $|I| < \log_2(|v(\mathcal{M})| + 1)$,

(ii) for each pair of distinct points $x, y \in v(\mathcal{M})$ there exists an $i \in I$ with $|(B_i \cap \{x, y\})| = 1$.

Clearly, there exists a family with properties (i) and (ii) (because we can embed $v(\mathcal{M})$ into 2^I). For each $i \in I$ define the equivalence $\sim_i$ on M as follows:

$x \sim_i y$ iff either $x, y \in B_i$ or $x, y \in v(\mathcal{M}) - B_i$ or $x = y$. The infimum of $\sim_i$, $i \in I$ in the equivalence lattice of M is the identical relation. Further, by the properties of 3-nilpotent monoids, $\sim_i$ is a congruence on $\mathcal{M}$ for each $i \in I$. Put $\mathcal{M}_i = \mathcal{M}/\sim_i$. Then by the well-known properties of subdirect product, $\mathcal{M}$ is subdirect product of the $\mathcal{M}_i$, $i \in I$ (see, e.g., [4, 10]). Thus (a) and (b) hold. Moreover $v(\mathcal{M}_i) = v(\mathcal{M})/\sim_i$ and so $|v(\mathcal{M}_i)| = 2$—thus (c) is true. Finally (d) follows from the fact that $|M_i| = |M| - |v(\mathcal{M})| + 2$.

THEOREM 3.10. $N(n) \leqslant 12n \log_2 n + n$.

The proof of this theorem follows from Propositions 3.1 and 3.8, Lemmas 2.3 and 3.9, and Theorem 1.10.

IV. REPRESENTATING MONOIDS BY HYPERGRAPHS

THEOREM 4.1. *For each $k \geqslant 3$ and $n \geqslant 6k + 6$, $M_k(n) \leqslant 2n + f(n)$, where $f(n)$ is the minimal positive integer such that $\binom{f(n)}{k-2} \geqslant n$. Thus $M_k(n) \leqslant 3n$.*

Proof. Let $\mathcal{M} = (M, \cdot, 1)$ be a monoid. Let (Y, S) be a rigid hypergraph such that $|Y| = f(|M|)$ and for each pair of points $x, y \in Y$ there exists a $(k+1)$-path from x to y (see Lemma 2.1). Choose a $(k-1)$ element set B of Y such that B is not a subset of any $C \in S$. Choose a $(k-2)$ element set A

in Y such that A is not a subset of B and choose a one-to-one mapping μ from M to the set of $(k-2)$ element subsets of Y with $\mu(1)=A$ (μ exists because $|Y|=f(|M|)$). Define $X=Y\cup(M\times\{0,1\})$ (assume $Y\cap(M\times\{0,1\})=\emptyset$), $T=S\cup\{\{(x,0),\ (yx,1)\}\cup\{\mu(y);\ x,y\in M\}\cup\{\{(x,0)\}\cup B; x\in M\}$. We prove that $\varphi: X\to X$ is an endomorphism of (X,T) iff

(a) $\varphi(Y)\subset Y$ and φ restricted to Y is the identity mapping of Y;

(b) there exists a right translation ψ of $\mathcal{M}$ such that $\varphi(x,i)=(\psi(x),i)$ for each $x\in M$, $i\in\{0,1\}$.

Thus the endomorphism monoid of (X,T) is isomorphic to $\mathcal{M}$ and so the proof will be complete.

Assume that $\varphi: X\to X$ is an endomorphism of (X,T). Then φ preserves $(k+1)$-paths and so $\varphi(Y)\subset Y$. Because (Y,S) is rigid we get that φ/Y is the identity mapping. Thus $\varphi(B)=B$ and hence $\varphi(M\times\{0\})\subset M\times\{0\}$. Further $\varphi(A)=A$ and therefore there exists $\psi: M\to M$ such that $\varphi(x,i)=(\psi(x),i)$ for each $x\in M$, $i\in\{0,1\}$. For $y\in M-\{1\}$ we have $\varphi(\mu(y))=\mu(y)$ and hence for each $x\in M$ $\varphi(\{(x,0),\ (yx,1)\}\cup\mu(y))=\{(\psi(x),0),\ (\psi(yx),1)\}\cup\mu(y)$. Because φ is an endomorphism we have $\psi(yx)=y\psi(x)$; thus ψ commutes with any left translation of $\mathcal{M}$ and so ψ is a right translation of $\mathcal{M}$.

On the other hand if φ fulfils (a) and (b) then it suffices to realize that $\varphi(\{(x,0),\ (yx,1)\}\cup\mu(y))=\{(\psi(x),0),\ (\psi(yx),1)\}\cup\mu(y)=\{(\psi(x),0),(y\psi(x),1)\}\cup\mu(y)$ because ψ commutes with any left translation of $\mathcal{M}$—the rest is obvious.

Remark 4.2. It is folklore, that any transformation monoid on an n-element set can be represented by an n-ary relation. For, if M acts on $V=\{v_1,\ldots,v_n\}$ then let $R=\{(\varphi v_1,\ldots,\varphi v_n);\ \varphi\in M\}$. Clearly, $\mathrm{End}(V,R)=M$. This, in particular, implies that every abstract monoid of order n can be represented by an n-set with an n-ary relation.

ACKNOWLEDGMENTS

We are deeply indebted to the references for many valuable remarks which improved the presentation of the material.

REFERENCES

1. L. BABAI, On the minimum order of graphs with given group, *Canad. Math. Bull.* **17** (1974), 467–470.
2. L. BABAI, Infinite digraphs with given regular automorphism groups, *J. Combin. Theory B* **25** (1978), 26–46.

3. L. BABAI, On the abstract group of automorphisms, *in* "Combinatorics, Proc. 8th British Comb. Conf., Swansea 1981," London Math. Soc. Lect. Notes, Vol. 52, pp. 1–40. Cambridge Univ. Press, London, 1981.
4. G. BIRKHOFF, Subdirect unions in universal algebra, *Bull. Amer Math. Soc.* **50** (1944), 764–768.
5. H. CHERNOFF, A measure of asymptotic efficiency for test of a hypothesis based on the sum of observations, *Ann. Math. Statist.* **23** (1952), 493–509.
6. A. H. CLIFFORD AND G. B. PRESTON, "Algebraic Theory of Semigroups," Amer. Math. Soc., Providence, R. I., 1964.
7. P. ERDŐS, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.* **53** (1947), 292–294.
8. P. ERDŐS AND A. RÉNYI, Assymmetric graphs, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 295–315.
9. P. ERDŐS AND J. H. SPENCER, "Probabilistic Methods in Combinatorics," Akadémiai Kiadó, Budapest, 1974.
10. G. GRÄTZER, "Universal Algebra," Princeton Univ. Press, Princeton, N. J., 1968.
11. Z. HEDRLÍN AND A. PULTR, Relations (graphs) with given finitely generated semigroups, *Monatsh. Math.* **68** (1964), 213–217.
12. P. HELL AND J. NEŠETŘIL, Graphs and k-societies, *Canad. Math. Bull.* **13** (1970), 375–381.
13. D. Y. KLEITMAN, B. P. ROTHSCHILD, AND J. H. SPENCER, The number of semigroups of order n, *Proc. Amer. Maath. Soc.* **55** (1976), 227–232.
14. V. KOUBEK AND V. RÖDL, On the number of monoids and groups of order n, manuscript, 1983.
15. L. LOVÁSZ, "Combinatorial Problems and Exercises," North-Holland, Amsterdam, 1979.
16. A. PULTR AND V. TRNKOVÁ, "Combinatorial, Algebraic and Topological Representations of Groups, Semigroups and Categories," North-Holland, Amsterdam, 1980.
17. E. SPENCER, Ein Satz über Untermenge einer endlichen Menge, *Math. Z.* **27** (1928), 544–548.